UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/605,189	09/12/2003	Gregor P. Freund	VIV/0011.01	2188

28653   7590   03/17/2010
JOHN A. SMART
201 LOS GATOS
SARATOGA RD, #161
LOS GATOS, CA 95030-5308

EXAMINER
TRUVAN, LEYNNA THANH

ART UNIT	PAPER NUMBER
2435	

MAIL DATE	DELIVERY MODE
03/17/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

	Application No.	Applicant(s)
Office Action Summary	10/605,189	FREUND, GREGOR P.
	Examiner	Art Unit	
	Leynna T. Truvan	2435	

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS,
WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>04 November 2009</u>.

2a)☒ This action is **FINAL**.   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
   closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>1-47</u> is/are pending in the application.

   4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>1-47</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

   Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

   Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   a)☐ All   b)☐ Some * c)☐ None of:

   1.☐ Certified copies of the priority documents have been received.

   2.☐ Certified copies of the priority documents have been received in Application No. _____.

   3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
      application from the International Bureau (PCT Rule 17.2(a)).

   * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO/SB/08)
     Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
     Paper No(s)/Mail Date. _____.

5)☐ Notice of Informal Patent Application

6)☐ Other: _____.

DETAILED ACTION

1.   Claims 1-47 are pending.

Response to Arguments

2.   Applicant's arguments with respect to claim 1-47 have been considered
but are moot in view of the new ground(s) of rejection.

     In the previous rejection, Ablay was the primary art. Currently due to
the amendment, Aaron is now the primary art and Ablay as secondary. Aaron
discloses the claimed invention including a system services of the operating system are
monitored for preventing indirect access to the computer network and Ablay is now
relied on to teach defining rules. Hence, Aaron discloses security in the form of
preventing indirect access to the system network **(col.8, lines 29-35 and col.12, lines
43-67).** Therefore, it would have been obvious for a person of ordinary skills in the art at
the time of the invention to combine the teachings of Aaron with Ablay to teach rules
indicating which system services a given application are monitored for preventing
indirect access to the computer network because to provide the service within the
system securely (Ablay - col.3, lines 17-23).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set
forth in section 102 of this title, if the differences between the subject matter sought to be patented and
the prior art are such that the subject matter as a whole would have been obvious at the time the
invention was made to a person having ordinary skill in the art to which said subject matter pertains.
Patentability shall not be negatived by the manner in which the invention was made.

3.   **Claims 1-47 are rejected under 35 U.S.C. 103(a) as being unpatentable over**

Aaron, et al. (US 7,509,675) in view of Ablay, et al. (US 6,002,941).

As per claim 1:

Aaron discloses in a computer system operating under control of an operating

system, a method for controlling <u>indirect access to a computer network by applications</u>

executing on the computer system, the method comprising:

[*defining rules*] indicating which system services of the operating system <u>are</u>

<u>monitored for preventing indirect access to the computer network</u>; **(col.8, lines 29-35**

and col.12, lines 43-67)

trapping an attempt to invoke a particular system service<u> being monitored</u>; **(col.5,**

lines 30-48)

<u>determining if the attempt to invoke the particular system service constitutes an</u>

<u>attempt by an unauthorized application to obtain indirect access to the computer</u>

<u>network by invoking the particular system service which in turn accesses the computer</u>

<u>network on behalf of the unauthorized application; and</u> **(col.8, lines 44-58 and col.10,**

lines 58-63)

if the attempt to invoke the particular system service constitutes an attempt by an unauthorized application to access the computer network indirectly, blocking the attempt. **(col.5, lines 14-25 and col.13, lines 12-25)**

Although, Aaron discloses system services of the operating system are monitored for preventing indirect access to the computer network but did not include defining rules.

Ablay discloses the service environment can be embodied within a stand alone computer (col.3, lines 20-28) and a Windows NT operating system was used to provide the service creation environment (col.4, lines 20-31). Ablay also discusses the computer operating system must provide interoperability between the higher-level applications and the underlying computer hardware (col.5, lines 30-35) based on rules (col.9, lines 14-40). Thus, shows the operating system of a computer system supports interprocess communication that invokes service according to an application rule in a computer system. Ablay discloses a service creation environment is used to create logic program rules based on at least one service building block. The logic program rules indicate identification of an authorized service execution environment where any of the at least one service building block used in the logic program rules can be configured to be responsive to at least one predetermined stimulus. Ablay states that each time the logic program rules for a service are invoked in the execution environment by receipt of the predetermined stimulus is term an instance of the service (col.2, line - col.3, line 20).

Therefore, it would have been obvious for a person of ordinary skills in the art at the time of the invention to combine the teachings of Aaron with Ablay to teach rules

indicating which system services a given application are monitored for preventing

indirect access to the computer network because to provide the service within the

system securely (Ablay - col.3, lines 17-23).

As per claim 2:   See Aaron on col.8, lines 44-58 and col.10, lines 58-63; discussing

the method of claim 1, wherein said trapping step includes intercepting operating

system calls for invoking the particular system service.

As per claim 3:   See Aaron on col.5, lines 30-48; discussing the method of claim 1,

wherein said trapping step includes intercepting local procedure calls for invoking the

particular system service.

As per claim 4: See Aaron on col.5, lines 1-48 and Ablay on col.3, lines 13-22 and col.4,

lines 34-52; discussing the method of claim 1, wherein said trapping step includes

intercepting an attempt to open a communication channel to the particular system

service.

As per claim 5: See Aaron on col.5, lines 14-25 and col.13, lines 12-25; discussing the

method of claim 1, wherein said trapping step includes rerouting an attempt to invoke

the particular system service from a system dispatch table to an interprocess

communication controller for determining whether to block the attempt based on the

rules.

As per claim 6:   See Aaron on col.8, lines 15-42 and col.13, lines 12-25; discussing

the method of claim 5, wherein said step of rerouting attempts to invoke the particular

system service from a dispatch table to the interprocess communication controller

includes replacing an original destination address in the system dispatch table with an

address of the interprocess communication controller.

As per claim 7: See Ablay on col.5, lines 14-25 and col.13, lines 12-25; discussing the method of claim 6, further comprising the steps of: retaining the original destination address; and using the original destination address for invoking the particular system service if the interprocess communication controller determines not to block the attempt.

As per claim 8: See Aaron on col.3, lines 50-55 and Ablay on col.3, lines 40-55 and 45-47; discussing the method of claim 1, wherein the rules specifying which system services are monitored are established based on user input.

As per claim 9: See Ablay on col.3, lines 52-55; discussing the method of claim 1, wherein the step of blocking the attempt is based upon consulting a rules engine for determining application authorized to invoke the particular system service.

As per claim 10:   See Aaron on col.3, lines 50-55 and col.13, lines 12-25; discussing the method of claim 1, wherein the step of blocking the attempt includes obtaining user input as to whether the unauthorized application should allow now be authorized to invoke the particular service.

As per claim 11: See Aaron on col.3, lines 50-55 and Ablay on col.6, lines 1-7; discussing the method of claim 10, wherein said step of obtaining user input includes the substeps of: providing information to the user about which particular application that is attempting to invoke the particular system service; and receiving user input as to whether the particular application should be blocked from invoking the particular system service.

As per claim 12: See col.11, lines 17-24; discussing the computer-readable medium

having computer-executable instructions for performing the method of claim 1.

As per claim 13: See col.11, lines 17-24 and col.13, lines 12-25; discussing

downloading a set of computer-executable instructions for performing the method of

claim 1.

As per claim 14:

Ablay discloses in a computer system operating under control of an operating

system, a method for regulating indirect access to the Internet, the method comprising:

defining a policy specifying processes authorized to access the Internet; **(col.8,**

lines 29-35 and col.12, lines 43-67)

intercepting an attempt by a first process to communicate with a second process

in a manner that provides the first process with indirect access to Internet; **(col.5, lines**

30-48)

identifying the first process that is attempting to communicate with the second

process; identifying the second process; **(col.14, lines 10-20)**

based on said policy, determining whether the first process may communicate

with the second process in a manner that provides the first process with indirect access

to Internet; and **(col.8, lines 44-58 and col.10, lines 58-63)**

allowing the first process to communicate with the second process if said policy

indicates that the first process may communicate with the second process in a manner

that provides the first process with indirect access to Internet. **(col.5, lines 14-25 and**

col.13, lines 12-25)

Although, Aaron includes specifying processes authorized to access the Internet.
but did not clearly suggest defining a policy specifying processes authorized to access
the Internet.

Ablay discloses the service environment can be embodied within a stand alone
computer (col.3, lines 20-28) and a Windows NT operating system was used to provide
the service creation environment (col.4, lines 20-31). Ablay also discusses the computer
operating system must provide interoperability between the higher-level applications
and the underlying computer hardware (col.5, lines 30-35) based on rules (col.9, lines
14-40). Thus, shows the operating system of a computer system supports interprocess
communication that invokes service according to an application rule in a computer
system. Ablay discloses a service creation environment is used to create logic program
rules based on at least one service building block. The logic program rules indicate
identification of an authorized service execution environment where any of the at least
one service building block used in the logic program rules can be configured to be
responsive to at least one predetermined stimulus. Ablay states that each time the logic
program rules for a service are invoked in the execution environment by receipt of the
predetermined stimulus is term an instance of the service (col.2, line - col.3, line 20).

Therefore, it would have been obvious for a person of ordinary skills in the art at
the time of the invention to combine the teachings of Aaron with Ablay to teach defining
a policy specifying processes authorized to access the Internet because to provide the
service within the system securely (Ablay - col.3, lines 17-23).

As per claim 15:   See Ablay on col.5, lines 30-67 and col.12, lines 39-60; discussing

the method of claim 14, wherein the first process comprises an instance of an
application program.

As per claim 16: See Ablay on col.5, lines 30-67 and col.12, lines 39-60; discussing the
method of claim 14, wherein the second process comprises a system service.

As per claim 17:   See Aaron on col.5, lines 30-48 and Ablay on col.5, lines 30-67 and
col.12, lines 39-60; discussing the method of claim 14, wherein said intercepting step
includes intercepting operating system calls made by the first process to attempt to
communicate with the second process.

As per claim 18:   See Aaron on col.5, lines 1-48 and Ablay on col.5, lines 30-67 and
col.12, lines 39-60; discussing the method of claim 14, wherein said intercepting step
includes detecting local procedure calls.

As per claim 19: See Ablay on col.5, lines 30-67 and col.12, lines 39-60; discussing the
method of claim 14, wherein said intercepting step includes detecting an attempt by the
first process to open a communication channel to the second process.

As per claim 20:   See Aaron on col.8, lines 15-42 and col.13, lines 12-25 and Ablay
on col.5, lines 30-67 and col.12, lines 39-60; discussing the method of claim 14, wherein
said intercepting step includes rerouting attempts by the first process to communicate
with the second process from a system dispatch table to an interprocess communication
controller.

As per claim 21:   See Aaron on col.5, lines 14-25 and col.13, lines 12-25 col.14, lines
1-9 and Ablay on col.5, lines 30-67 and col.12, lines 39-60; discussing the method of
claim 14, wherein said step of identifying the second process includes evaluating

parameters of the attempt made by the first process to communicate with the second

process.

As per claim 22:   See Ablay on col.5, lines 30-67 and col.12, lines 39-60; discussing

the method of claim 14, wherein said policy specifies particular processes to be

protected from communications made by other processes.

As per claim 23:   See Ablay on col.5, lines 30-67 and col.12, lines 39-60; discussing

the method of claim 14, further comprising: providing for a process to be registered in

order to be protected from communications made by other processes; and determining

whether to allow the first process to communicate with the second process based, at

least in part, upon determining whether the second process is registered.

As per claim 24: See Aaron on col.8, lines 15-42 and col.13, lines 12-25 and col.14,

lines 1-9 and Ablay on; discussing the method of claim 23, wherein said determining

step is based, at least in part, on the type of communication the first process is

attempting with the second process.

As per claim 25:

        Dugan discloses in a computer system operating under control of an operating

system, a method for <u>preventing one application from gaining indirect Internet access</u>

<u>through other applications</u>, the method comprising:

        registering a first application to be protected from <u>serving as a proxy by which</u>

<u>other applications may gain indirect Internet access</u>; **(col.8, lines 12-35 and col.12,**

lines 43-67)

detecting an attempt to access the first application for purposes of using the first

application as proxy for indirect Internet access; **(col.5, lines 30-48)**

identifying a second application that is attempting to access the first application

for purpose of using the first application as a proxy for indirect Internet access; and

(col.8, lines 44-58 and col.10, lines 58-63)

rerouting the attempt to access the first application through an interprocess

communication controller that determines whether to allow the attempt, based on rules

indicating whether the second application is authorized access the first application using

interprocess communication. **(col.5, lines 14-25 and col.13, lines 12-25)**

However, Aaron did not include rules indicating whether the second application is

authorized access the first application using interprocess communication.

Ablay discloses the service environment can be embodied within a stand alone

computer (col.3, lines 20-28) and a Windows NT operating system was used to provide

the service creation environment (col.4, lines 20-31). Ablay also discusses the computer

operating system must provide interoperability between the higher-level applications

and the underlying computer hardware (col.5, lines 30-35) based on rules (col.9, lines

14-40). Thus, shows the operating system of a computer system supports interprocess

communication that invokes service according to an application rule in a computer

system. Ablay discloses a service creation environment is used to create logic program

rules based on at least one service building block. The logic program rules indicate

identification of an authorized service execution environment where any of the at least

one service building block used in the logic program rules can be configured to be

responsive to at least one predetermined stimulus. Ablay states that each time the logic

program rules for a service are invoked in the execution environment by receipt of the

predetermined stimulus is term an instance of the service (col.2, line - col.3, line 20).

      Therefore, it would have been obvious for a person of ordinary skills in the art at

the time of the invention to combine the teachings of Aaron with Ablay to teach rules

indicating whether the second application is authorized access the first application using

interprocess communication because to provide the service within the system securely

(Ablay - col.3, lines 17-23).

As per claim 26:   See Ablay on col.3, lines 13-28 and col.8, lines 1-7 and 53-67;

discussing the method of claim 25, wherein said registering step includes supplying

rules specifying particular communications from which the first application is to be

protected.

As per claim 27:   See Ablay on col.3, lines 13-28 and col.8, lines 1-7 and 53-67;

discussing the method of claim 26, wherein the interprocess communication controller

determines whether to allow the attempt based, at least in part, upon the rules

specifying particular communications from which the first application is to be protected.

As per claim 28:   See Aaron on col.5, lines 1-48; discussing the method of claim 25,

wherein said detecting step includes intercepting operating system calls for accessing

the first application.

As per claim 29:   See Aaron on col.11, lines 3-16 and Ablay on col.3, lines 60-63 and

col.6, lines 10-15; discussing the method of claim 25, wherein said detecting step

includes detecting a graphical device interface (GDI) message sent to the first

application.

As per claim 30:   See Aaron on col.11, lines 3-16 and Ablay on col.3, lines 13-28 and

col.8, lines 1-7 and 53-67; discussing the method of claim 29, wherein said identifying

step includes evaluating parameters of the message sent to the first application.

As per claim 31:   See Ablay on col.3, lines 13-28 and col.8, lines 1-7 and 53-67;

discussing the method of claim 25, wherein said detecting step includes detecting an

attempt to send keystroke data to a window of the first application.

As per claim 32:   See Ablay on col.3, lines 13-28 and col.8, lines 1-7 and 53-67;

discussing the method of claim 25, wherein said detecting step includes detecting an

attempt to send mouse movement data to a window of the first application.

As per claim 33:   See Aaron on col.8, lines 15-42 and col.13, lines 12-25 and Ablay

on col.5, lines 30-67 and col.12, lines 39-60; discussing the method of claim 25, wherein

said rerouting step includes rerouting the attempt to access the first application from a

system dispatch table to the interprocess communication controller.

As per claim 34: See Ablay on col.5, lines 30-67 and col.12, lines 39-60; discussing the

method of claim 25, wherein said rules indicating whether the second application may

access the first application includes rules indicating particular types of communications

which are allowed.

As per claim 35:   See Aaron on col.11, lines 3-16 and Ablay on col.5, lines 30-67 and

col.12, lines 39-60; discussing the method of claim 25, further comprising: if the

interprocess communication controller allows the attempt to access the first application,

routing the attempt to the first application.

As per claim 36:

Ablay discloses a system for regulating <u>Internet access by controlling</u> interprocess communication between applications, the system comprising:

a computer having at least one process, said computer system operating under control of an operating system supporting interprocess communication;

a policy specifying applications that are permitted to communicate with a first application using interprocess communication<u>, said first application capable of providing indirect Internet access to other applications</u>; **(col.8, lines 29-35 and col.12, lines 43-67)**

a module for detecting <u>an attempt by</u> a second application <u>gaining indirect Internet access through</u> the first application using interprocess communication; and **(col.5, lines 30-48)**

an interprocess communication controller for identifying the second application attempting to <u>gaining indirect Internet access through</u> the first application <u>using interprocess communication</u> **(col.8, lines 44-58 and col.10, lines 58-63)** and determining whether to permit the communication based upon the identification of the second application and the policy specifying applications permitted to communicate with the first application. **(col.5, lines 14-25 and col.13, lines 12-25)**

Although, Aaron includes applications permitted to communicate with a first application using interprocess communication. However, Aaron did not include a policy specifying applications that are permitted to communicate with a first application.

Ablay discloses the service environment can be embodied within a stand alone computer (col.3, lines 20-28) and a Windows NT operating system was used to provide the service creation environment (col.4, lines 20-31). Ablay also discusses the computer operating system must provide interoperability between the higher-level applications and the underlying computer hardware (col.5, lines 30-35) based on rules (col.9, lines 14-40). Thus, shows the operating system of a computer system supports interprocess communication that invokes service according to an application rule in a computer system. Ablay discloses a service creation environment is used to create logic program rules based on at least one service building block. The logic program rules indicate identification of an authorized service execution environment where any of the at least one service building block used in the logic program rules can be configured to be responsive to at least one predetermined stimulus. Ablay states that each time the logic program rules for a service are invoked in the execution environment by receipt of the predetermined stimulus is term an instance of the service (col.2, line - col.3, line 20).

Therefore, it would have been obvious for a person of ordinary skills in the art at the time of the invention to combine the teachings of Aaron with Ablay to teach a policy specifying applications that are permitted to communicate with a first application because to provide the service within the system securely (Ablay - col.3, lines 17-23).

As per claim 37:   See Ablay on col.3, lines 13-28 and col.8, lines 1-7 and 53-67; discussing the system of claim 36, wherein said policy includes rules indicating particular types of communications which are permitted.

As per claim 38:   See Ablay on col.3, lines 13-28 and col.8, lines 1-7 and 53-67;

discussing the system of claim 36, further comprising: a rules engine for specifying applications that are permitted to communicate with the first application using interprocess communication.

As per claim 39:   See Ablay on col.4, lines 32-65 and col.5, lines 50-65; discussing the system of claim 36, further comprising: a registration module for establishing said policy.

As per claim 40:   See Ablay on col.4, lines 32-65 and col.5, lines 50-65; discussing the system of claim 39, wherein said registration module provides for identifying applications to be governed by said policy.

As per claim 41:   See col.5, lines 14-25 and Ablay on col.3, lines 1-21 and col.5, lines 50-65; discussing the system of claim 36, wherein said module for detecting a second application detects an operating system call to open a communication channel to the first application.

As per claim 42:   See Aaron on col.11, lines 3-16 and Ablay on col.3, lines 1-21 and col.12, lines 39-60; discussing the system of claim 36, wherein said module for detecting a second application detects a graphical device interface (GDI) message sent to the first application.

As per claim 43:   See Aaron on col.5, lines 14-25 and col.13, lines 12-25 and Ablay on col.3, lines 1-21 and col.5, lines 50-65; discussing the system of claim 36, wherein said module for detecting a second application detects a local procedure call attempting to access the first application.

As per claim 44:   See Aaron on col.8, lines 15-42 and col.13, lines 12-25 and Ablay

on col.3, lines 1-21 and col.8, lines 1-7 and 53-67; discussing the system of claim 36, wherein said module for detecting a second application redirects attempts to communicate with the first application to the interprocess communication controller.

As per claim 45:   See Aaron on col.8, lines 15-42 and col.13, lines 12-25 and Ablay on col.3, lines 13-28 and col.8, lines 1-7 and 53-67; discussing the system of claim 36, wherein said module for detecting a second application reroutes the attempt to communicate with the first application from a dispatch table to the interprocess communication controller.

As per claim 46:   See Aaron on col.11, lines 3-16 and Ablay on col.3, lines 13-28 and col.8, lines 1-7 and 53-67; discussing the system of claim 36, wherein said interprocess communication controller determines whether to permit the communication based, at least in part, upon evaluating parameters of the attempt made by the second application to communicate with the first application.

As per claim 47:   See Aaron on col.3, lines 50-55 and Ablay on discussing the system of claim 36, wherein said interprocess communication controller determines whether to permit the communication based upon obtaining user input as to whether to permit the second application to communicate with the first application.

Conclusion

4.   Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**.

See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Leynna T. Truvan whose telephone number is (571) 272-3851. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR

only. For more information about the PAIR system, see http://pair-direct.uspto.gov.

Should you have questions on access to the Private PAIR system, contact the

Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like

assistance from a USPTO Customer Service Representative or access to the automated

information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/L. T. T./
Examiner, Art Unit 2435
        /Kimyen Vu/
        Supervisory Patent Examiner, Art Unit 2435